Security Awareness Training for Third-Party Risk Management

Third-party risk management is important to your organization's overall risk management strategy. When you manage third-party risks effectively, you minimize the potential for a data breach occurring as a result of working with other companies or organizations.

Securing your organization's ecosystem, including your third-party contractors and supply chain, is one of the most important and challenging aspects of risk management.

The best way to minimize risk and strengthen your information security. Effective awareness training for all your business units worldwide.

REQUEST MY DEMO

WHAT IS TPRM? | FRAMEWORKS | EXAMPLES | ELEMENTS OF TPRM

What Is Third-Party Risk Management (TPRM)?

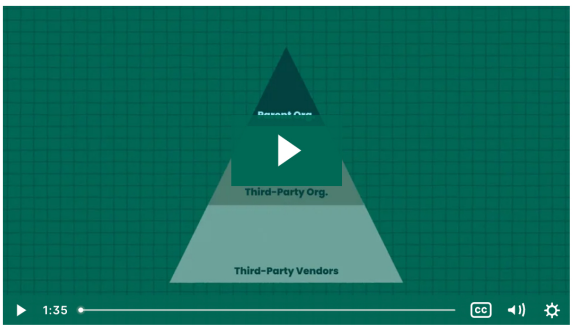
Third-party risk management (TPRM) is the process of identifying, assessing, and managing the risks associated with outsourcing work to a third party. These can include partners, resellers, contractors, suppliers, and other entities.

Related policies or practices, such as vendor risk management or service provider management, are subsets of third-party risk management.

The goal of third-party risk management is to ensure you're not accidentally exposing yourself or your organization to unnecessary risks by allowing access to systems and data to external contractors, suppliers, or other service providers. You want to make sure that you're being proactive and thinking through every possible scenario from a cyber security perspective.

Reducing third-party risk factors involves much more than implementing technical guardrails, such as firewalls and email security infrastructure. The vast majority of data breaches occur because of human error, making it a crucial line of defense against all cyber threats.

As a result, strong security awareness training can mean the difference between leaving sensitive information vulnerable and keeping it out of the hands of hackers.



Why Is Third-Party Risk Management Important?

Third-party risk management is crucial because it ensures that your company doesn't take on unnecessary or uncontrollable risks by outsourcing work to third-party entities. It also helps ensure that your company complies with security and data privacy regulations like GDPR and SOC 2 audits.

If a company's supply chain is left unguarded or lacks overall visibility into

If a company's supply chain is left ungoverned or lacks overall visibility into each business unit's cyber security practices, it can be its Achilles' heel, especially regarding TPRM. In the event of a supplier or vendor data breach, the organization will likely experience service downtime and many other tech-related issues.

Those scenarios can culminate in hours, days, or weeks' worth of downtime, which results in major operational disruptions and significant long-term revenue losses. Beyond these considerations, an organization can see irreparable damage to its brand, as consumers will likely view it as less trustworthy after a data breach.

When a data breach occurs, even if caused by a supplier or another third party, your organization is still responsible for managing the event's fallout.

These consequences can be avoided by investing in security awareness training and ensuring all third parties and an organization's core employees consistently adhere to safe online behaviors when handling sensitive information.

Who is responsible for third-party risk management?

Third-party risk management typically falls under the purview of IT or Risk Management teams. A risk management policy should document a framework for how these teams should manage third parties and related processes. The framework can vary from organization to organization – what's important to that the information is communicated to all parties.

While the responsibility for managing third-party risk lies chiefly with IT and Risk Management teams, every employee and third-party contractor plays a part in keeping sensitive information secure. Everyone needs to understand this and how it impacts their organizational role.

What is the best TPRM framework?

There are many known frameworks available for managing third-party risks. One example is ISO/IEC 27001:2022, which includes a framework for integrating risk management into an organization's overall information security management system (ISMS) via Annex A.15: Supplier Relationship.

The ISO/IEC 27036-1:2021 Cyber security — Supplier relationships standard guides to assist organizations in securing their systems and data within the context of supplier relationships.

TPRM is vital to your organization's overall risk management strategy. When you manage third-party risks, you protect your organization from the risks associated with working with other companies or organizations.

Regardless of your chosen framework, it's essential to consider whether your organization is well-prepared for a potential cyber attack.

What is your capacity to detect and respond? Can you keep essential business services and systems running during an incident? How quickly can you recover from a cyber incident?

By painting a detailed picture of your organization's reality via a risk assessment, you'll be able to build a robust risk management framework and select the right awareness training to minimize the human risk factor.

To complete a risk assessment, you must:

IDENTIFY	DEFINE	EVALUATE
Identify the assets that require protection and their value	**Define** both the risk and threat and identify the cyber attack surface	**Evaluate** whether the proper controls and safeguards are in place to protect crucial assets in the most efficient way

To get the insight you need to develop your risk management framework and corresponding strategy, Terranova Security CISOs recommend asking the following questions:

1. What assets are you trying to protect? What's their value?
2. Did you identify attack vectors and potential cyber threats?
3. Do you have the proper controls in place to safeguard the assets identified in Question 1?
4. Did you conduct a full risk assessment and identify your risk appetite?
5. Did you evaluate your existing safeguards and pinpoint gaps between your current standing and your organization's risk management goals?

Once complete, you'll have clear insight into your organization's cyber security maturity level. With that intel, you can gauge how resilient you are to cyber threats and easily craft an action plan to ensure all employees and third-party business units can detect and report potential attacks.

To strengthen information security, you can't rely solely on technological safeguards. Implementing ongoing security awareness training campaigns targeting the correct risk areas is crucial to long-term success.

Third-party risk management is vital to your organization's overall risk management strategy. When you manage third-party risks, you protect your organization from the risks associated with working with other companies or organizations.

Third-party risk management vs. Vendor risk management

Third-party risk management refers to processes, policies, and controls to manage risks associated with working with third parties. It is distinct from vendor risk management, which only focuses on managing risks with vendors.

Third-party risk management is a more global term. It focuses on identifying and addressing risks connected with all third parties who are part of an organization's business ecosystem.

Third parties can include vendors, suppliers, service providers, partners, contractors, and anyone with access to an organization's proprietary systems or data.

Vendor risk management is a critical element of third-party risk management, mainly when an organization relies on technology, service providers, or other suppliers to achieve business objectives. Strong vendor risk management helps minimize potential disruptions in those workflows or the introduction of additional risks.

Third-party risk management examples

There are many examples of third-party risk management considerations and how they can impact your organization. Various factors will influence your security team's direction, such as resources, scope, regional distribution, and how much third-party outsourcing is leveraged to attain business objectives.

Regardless of your organization's reality, all security and business leaders must consider risk areas that can be amplified by increased reliance on third-party outsourcing.

Some common examples of third-party risk factors include:

- Cyber security risk
- Regulatory/compliance risk
- Financial risk
- Operational risk
- Reputational risk

When you incorporate a third party into your business operations, you also add a potential conduit for a breach. This causes you to unknowingly take numerous forms of risk, especially in terms of cyber security.

To ensure all parties keep cyber security best practices in mind, implementing a security awareness training program that educates all business units on unsafe online behaviors is imperative.

How to Use Third-Party Risk Management to Sidestep Data Breaches

Because of its importance to overall cyber security and data privacy compliance, an organization must be able to rely on its third-party risk management processes and standards across all its business units. However, there's no one-size-fits-all formula for success.

As a result, a successful TPRM policy or process can be comprised of several different tactics. Like risk factors and resource allocation, your strategy may depart from those used by other organizations in your region or industry.

Some essential elements of TPRM you should consider are:

Evaluation

Evaluating the security and data protection practices of third parties before entering contracts with them or sharing information. This may be done via questionnaires or requests for audit reports.

Continuous monitoring

Regularly monitor third parties' security and compliance posture to identify potential risks and ensure ongoing compliance. This may be done via technology or manual verifications.

Incident response planning

Establishing a plan for responding to security incidents involving third parties, including communication protocols and escalation procedures. Having contact info and access to critical resources and the incident management team at the third party is crucial.

Contract review and negotiation

Carefully review and negotiate contracts and non-disclosure agreements with third parties to ensure adequate security and data protection provisions are in place. Establishing templates and requirements ahead of time can facilitate the process.

Cyber insurance

Purchasing cyber insurance to provide financial protection against losses due to third-party data breaches or other cyber incidents.

Reduce Third-Party Risk with Security Awareness Training

Working with third-party entities can potentially put your business at risk. Without TPRM that includes a cyber security awareness training aspect, contractors, suppliers, or vendors that fall into that category may unknowingly leave sensitive information vulnerable to hackers.

Minimizing the human risk factor starts with building a strong overall relationship with all stakeholders within your third-party vendor risk management framework. Additionally, investing in awareness training that changes end user behaviors for the better is the gateway to more robust data protection.

That's where Fortra's Terranova Security comes in. From providing engaging, informative training on the latest cyber threats to ensuring your program implementation is quick and seamless, we'll help you secure your entire business ecosystem and elevate your control over your cyber security infrastructure.

See the difference working with an industry-leading awareness training provider can make – book your personalized walkthrough today!

SCHEDULE MY DEMO

Continue Learning

BLOG

Risky Business: When Third-Party Troubles Become Your Own

READ MORE

BLOG

How to Enhance Third Party Risk Management with Cyber Security Training

READ MORE

BLOG

Why Your Third-Party Vendors Have Almost Definitely Been Breached and What to Do About It

READ MORE

BLOG

What's the Damage? The Truth About the Cost of Data Breaches

READ MORE

FORTRA

TRAINING

- Cyber Security Training for Employees
- Privacy Awareness
- Phishing Simulation
- Compliance & Governance
- Cyber Games

GET STARTED

- Platform Overview
- Free Demo
- Request a Quote
- Phishing Simulation Trial
- Guide to Security Awareness Training

COMPANY

- About Terranova Security
- Join Our Team
- Customer Support